E-Voting Verification

Zulkarnaim Masyhur[1], Budi Rahardjo[2]
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha No.10, Kota Bandung, Jawa Barat, Telp/ Fax: +62-22-250 0935
e-mail : [1]zulkarnaim.masyhur@gmail.com, [2]rahard@gmail.com

Abstrak *– Sistem pemungutan suara elektronik (e-voting) telah berkembang pesat dan menggantikan sistem pemungutan suara konvensional yang menggunakan kertas. Ada beberapa aspek yang mempengaruhi kepercayaan terhadap sistem pemungutan suara elektronik. Salah satu aspek vital yang harus diperhatikan dalam membuat sistem pemungutan suara elektronik adalah aspek verifikasi. Aspek verifikasi dikatakan vital sebab rendahya tingkat kepercaryaan pemilih dan kandidat yang rendah terhadap sistem pemungutan suara elektronik. Ada beberapa jenis verifikasi dalam sistem pemungutan suara elektronik yaitu individual verifiability, universal verifiability, dan elegibility verifiability. Penerapan jenis-jenis verifikasi tersebut pada sistem pemungutan suara JCJ/Civitas dan Helios yang telah dikembangkan akan direview dalam paper ini.*

Kata Kunci*: e-voting, verification, individual verifiability, universal verifiability, elegibilty verifiability.*

1. Pendahuluan

Tidak dapat terbantahkan bahwa dengan sistem pemungutan suara elektronik dapat memberikan banyak manfaat seperti meningkatkan akurasi, mempercepat operasi dan juga efesiensi biaya, tetapi pengimplementasian sistem ini berjalan lambat di beberapa negara karena adanya pro kontra dan perdebatan. Salah satu alasan yang mendasari hal tersebut ialah masih adanya kelemahan dari sistem e-voting sehingga sangat rentan terhadap manipulasi hasil akhir voting [1]. Granor dan Cytron (1997) merekomendasikan empat kriteria pokok dan tiga kategori teknis untuk sebuah sistem pemungutan suara yang ideal yaitu *accuracy*, *invulnerability*, *privacy* dan *verifiability* [2]. Faktor *verifiability* merupakan salah satu aspek yang mempengaruhi tingkat kepercayaan pemilih dan kandidat terhadap sistem penmungutan suara elektronik. Ketepatan dari sebuah sistem pemungutan suara diindikasikan dari aspek *verifiability* dimana pemilih dapat memverifikasi bahwa suaranya dapat mempengaruhi hasil pemilihan dan hasil dari pemilihan tersebut terdiri dari suara-suara yang diberikan oleh pemilih yang sah atau memiliki hak suara [3].

Verifikasi pemilihan pada *bulletin board* dapat dengan mudah dibagi dalam tiga pengertian [4]:

Individual Verifiability [5] harus memberikan kemungkinan kepada pemilih untuk memverifikasi bahwa surat suara yang dipilihnya telah tercatat dan terhitung oleh sistem dengan benar. Idealnya, pemilih juga harus memiliki jaminan bahwa surat suaranya telah melalui proses *encoding* dengan benar. Pada beberapa sistem adanya jaminan tambahan dengan menawarkan opsi audit terhadap surat suara [6] sebelum dilakukan proses perhitungan suara.

Universal Verifiability [7] harus memberikan kemungkinan untuk memverifikasi semua hasil pemilihan telah terhitung dengan benar. Siapapun dapat memverifikasi hasil yang telah diumumkan merupakan akumulasi yang benar dari hasil pemilihan setiap pemilih. [3] **Eligibility Verifiability** [8] harus memberikan kemungkinan untuk melakukan verifikasi

terhadap hasil pemilihan yang diambil dari surat suara yang telah dipilih oleh pemilih yang berhak. *Eligibility* dapat diterapkan pada setiap tahap pada sistem, baik selama proses pemungutan suara [9], proses perekaman hasil pemilihan ataupun pada proses perhitungan suara. Dengan demikian, *eligibility verifiability* akan mencakup tahap-tahap yang sesuai.

Dengan penerapan ketiga jenis verifikasi ini dapat memberikan jaminan bahwa pemungutan suara berjalan denga benar [3]. Satu masalah yang sering ditemui ialah pemilih tidak melakukan proses *indivual verifiability* pada *bulletin board* sistem pemungutan suara elektronik untuk memastikan bahwa surat suara pemilih tersebut tercatat dan terhitung dengan baik pada sistem pemungutan suara elektronik. Ini dapat ditemui pada sistem pemungutan suara Helios [10], Pret-a-Voter [9], JCJ/Civitas [11] dan sebagainya.

Pada pembahasan selanjutnya akan membahas beberapa jenis verifikasi yang telah diimplementasikan pada beberapa protokol sistem pemungutan suara dan memberikan analisis serta membahas kemungkinan-kemungkinan serangan yang dapat berdampak negatif pada beberapa jenis protokol sistem pemungutan suara tersebut khususnya yang berhubungan dengan aspek verifikasi.

2. Metode Penelitian

Pada peneltian kali ini menggunakan metode penelitian studi pustaka dan analisis. Studi pustaka dilakukan bertujuan untuk mengumpulkan informasi yang terkait langsung dengan teori-teori keilmuan yang menunjang, hasil-hasil penelitian yang sudah dipublikasikan untuk menjadi referensi dalam penelitian ini. Hal utama yang menjadi fokus dalam studi pustaka ini adalah aspek *verifiability* dari sistem pemungutan suara elektronik, jenis-jenis aspek *verifiability* serta penerapannya pada beberapa sistem pemungutan suara elektronik yang telah dikembangkan sebelumnya.

Pada aspek analisis diawali dengan memahami konsep verifikasi dari sistem pemungutan suara elektronik yang terkait dengan topik penelitian kali ini. Selanjutnya melakukan analisis terhadap penerapan jenis-jenis *verifiability* pada sistem-sistem pemungutan suara elektronik yang telah dikembangkan sebelumnya.

3. E-Voting Verifiability

Proses verifikasi pada sistem pemungutan suara sangatlah penting dikarenakan dengan adanya proses verifikasi hasil pemilihan dan perhitungan dapat dipertanggungjawabkan. Terlebih lagi jika sistem pemungutan suara digunakan dalam pemilihan yang melibatkan unsur politik, aspek verifikasi ini harus lebih diperhatikan lagi. Pada pendahuluan telah sempat dijelaskan perihal beberapa metode verifikasi pada sistem pemungutan suara seperti *individual verifiability, universal verifiability* dan *elegibility verifiability*. Dengan adanya sistem verifikasi yang bagus memungkinkan suara dapat disimpan pada pada perangkat yang diyakini kebenarannya dan dapat dihitung ulang untuk pembuktian bilamana diragukan kebenarannya. [2]

Adapun penerapan dari ketiga metode verifikasi yang telah disebutkan diatas akan direview dimana protokol yang akan digunakan adalah protokol JCJ/Civitas dan Helios dengan pertimbangan kedua protokol tersebut telah menerapkan ketiga metode verifikasi tersebut.

3.1. JCJ/Civitas Overview

Aspek utama dari JCJ/Civitas adalah terletak pada *credentials* dengan *public* dan *private part*, yang memungkinkan pemilih yang sah dapat mengautentikasi surat suaranya. JCJ/Civitas

ISBN: 978-602-60581-0-2

mendistribusikan *credential generation* di antara seperangkat *parties* yang dinamakan *registrars* untuk memungkinkan adanya coercion-resistance pada sistem pemungutan suara JCJ/Civitas. Diasumsikan bahwa setidaknya ada salah satu *registrar* yang tidak dirusak oleh coercer dan pemilih dapat berkomunikasi dengan registrars tersebut menggunakan sebuah untappable channel**.**

Adapun beberapa protokol yang ada pada sistem ini adalah

R – Seperangkat registrar yang mempunyai fungsi untuk melakukan autentikasi terhadap pemilih yag sah dan membangkitkan *credential* mereka.

T – Seperangkat *trustees* yang berfungsi untuk membangkitkan dan menerbitkan kunci publik dari pemilihan.

***V*1,...,*Vn*-** Merupakan pemilih yang sah

M - *re-encryption mix net*, yang berfungsi untuk menganonimkan surat suara sebelum memverifikasi keabsahan dan dekripsinya.

B - *the bulletin board*, yang berfungsinya untuk mencatat manipulasi surat suara pada semua tahapan pemilihan, dari pencatatan sampai proses perhitungan. [12]

3.2. JCJ/Civitas Verifiability

Universal verifiability dan *Eligibilty verifiability* pada JCJ/Civitas dapat dibuktikan dengan apa yang tertera pada *bulletin boards*:

- *Mix proofs* memungkinkan auditor untuk **A** untuk memverifikasi semua surat suara yang berasal dari mixnet **M**

- *PET proofs* dan *proofs Pcv* memungkinkan **A** untuk memverifikasi pemilihan dari pemilih yang sah dari yang tertera pada bulletin board untuk deskripsi terakhir

- *Decryption proofs* memungkinkan A untuk memverifikasi semua surat yang terhitung telah terdekrip dengan benar

Individual verifiability bisa dilakukan dengan mengikuti langkah-langkah berikut:

- **V** harus percaya mesin pemilihan tersebut dapat *encodes* surat suara yang telah dipilihnya dengan benar.

- **V** dapat mengecek *bulletin board* untuk melihat surat suaranya telah terekam dengan benar.

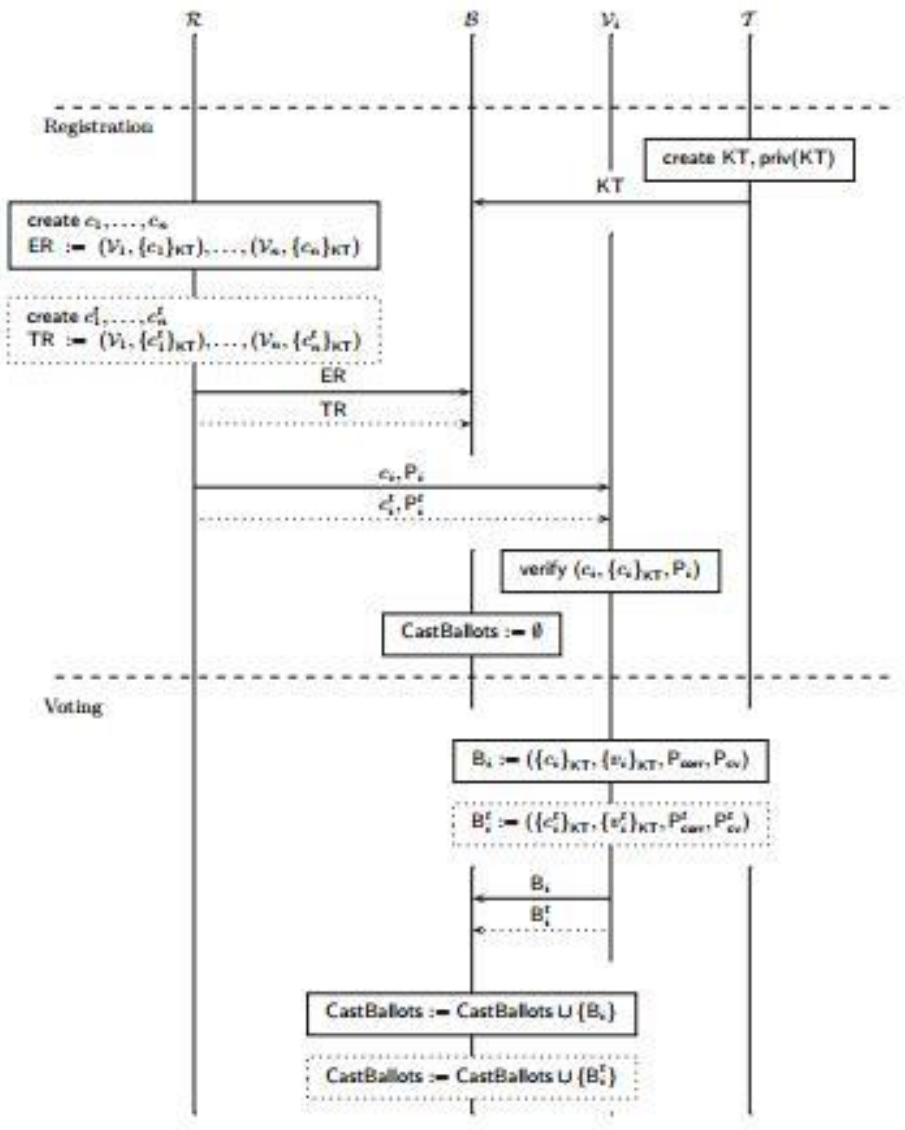
- *Universal verifiability* dari *Mix nets* memastikan bahwa semua hasil pemilihan telah *mixed* dengan benar dan suara yang telah dipilih ole **V** termasuk dalam kumpulan *mixed ballot.*

- *Universal verifiability of PETs* memastikan bahwa setidaknya ada 1 salinan dari surat suara V yang tersimpan setalah eliminasi dari duplikasi. *Proof Pi* yang memastikan bahwa pemilih mendapatkan *private credentials corresponds* untuk *public credentials*

ISBN: 978-602-60581-0-2

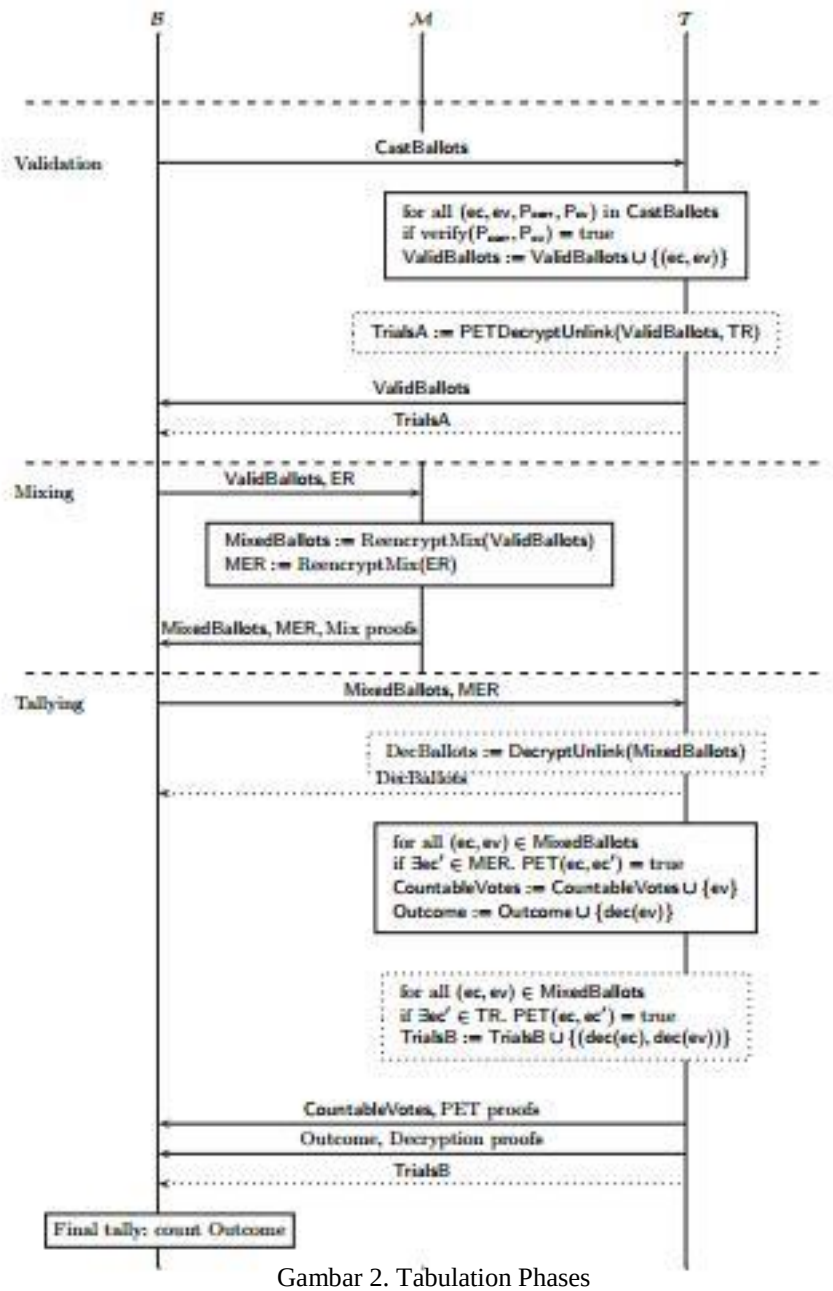
pada electoral roll **ER**. *Universal verifiability* dari *Mix nets* memastikan proses enkripsi ulang dari *public credentials* juga dihadirkan pada *anonymized electoral roll* **MER.**

Pada akhirnya, universal verifiability dari dekripsi yang terdistribusi memastikan bahwa surat suara **V** terdekrip dan terhitung dengan benar. [12]



Gambar 1. Registration and Voting Phases

ISBN: 978-602-60581-0-2



Gambar 2. Tabulation Phases

3.3. Overwiev Helios 2.0

Helios [13] merupakan sebuah sistem *open source* yang berbasis web *voting system* yang telah digunakan pada dunia nyata. International Association of Cryptologic Research (IACR) telah menggunakan Helios setiap tahunnya sejak 2010 untuk pemilihan *board member* [14]. The Catholic University of Louvaian menggunakan Helios untuk pemilihan rektor dan Princenton University menggunakan Helios untuk pemilihan mahasiswa pemerintah [13]. Helios dimaksudkan untuk memuaskan *verifiability* dan menjaga kerahasiaan dari surat suara. Untuk kerahasiaan surat suara, pemilih mengenkrip kandidat pilihan dengan skema enkripsi *homomorphic* dan untuk *verifiability*, proses enkripsi dan dekripsi dipadukan dengan *zero-knowledge proofs.* Adapun tahapan dari helios adalah

- Setup. *tallier* menghasilkan sepasang kunci untuk homomorphic skema enkripsi dan

ISBN: 978-602-60581-0-2

menerbitkan kunci publik

- Voting. Pemilih mengenkripsi pilihan kandidat nya dengan kunci publik *tallier* ini, dan zero-knowledge membuktikan bahwa ciphertext yang berisi pilihan terbentuk dengan baik.

- Tallying. *tallier* menyingkirkan surat suara terbukti tidak sah dari *buletin board*. *tallier* yang *homomorphically* menggabungkan *cipherteks* dalam surat suara yang tersisa, mendekripsi kombinasi *homomorphic*, dan membuktikan dalam zero-knowledge bahwa dekripsi dilakukan dengan benar. Akhirnya, *tallier* menerbitkan calon yang menang dan bukti dekripsi yang benar.

- Verification. *A verifier recomputes* kombinasi homomorphic dan memeriksa semua bukti zero-knowledge. [14]

Adanya celah keamanan yang ditemukan pada Helios 2.0 telah ditemukan antara lain :

- Verifiability exploits dikaitkan dengan penerapan transformasi Fiat-Shamir tanpa

  dimasukkannya statement ke dalam hash (i.e., the weak Fiat–Shamir transformation), dan termasuk pernyataan dalam hash (i.e., applying the Fiat–Shamir transformation) yang didalilkan sebagai pembelaan [15].

- Ballot secrecy exploits dikaitkan dengan menghitung-hitung suara terkait dan mengilangkan suara tersebut dari perhitungan yang didalilkan sebagai pembelaan [16]

3.4. Helios Verifiability

Pemilihan dibuat dengan penamaan satu set *trustees* dan menjalankan protokol yang menyediakan masing-masing bagian rahasia dari sepasang kunci public. Bagian umum dari kunci yang diterbitkan, setiap pemilih yang sah disediakan dnegan sebuah *private pseudi-identity.* Langkah-langkah yang dijalani partisipan selama berjalannya Helios [4] adalah

- Untuk memberikan vote, penguna menjalankan *script browser* untuk menginput pilihannya dan membuat suaranya dienckrip dengan kunci public dari pemilihan. Suara tersebut terdapat sebuah KZP yang merupakan indicator pemili yang sah.

- Pengguna dapat mengaudit surat suara untuk memeriksa apakah itu benar-benar mewakili suara dia dalam pemilihan. Jika dia memilih untuk melakukan ini, *script* akan menyediakan random data yang digunakan dalam pembuatan *ballot*.

Ketika pemilih telah memutuskan untuk memberikan suara nya, browser pemilih mengajukan bersama dengan dia pseudo-identitas ke server. Server memeriksa ZKPs dari surat suara, dan menerbitkan mereka di bulletin board.

- Pemilih individu dapat memeriksa bahwa suara mereka muncul di bulletin board. Pengamat dapat memeriksa bahwa surat suara yang muncul di papan pengumuman mewakili pemilih yang sah, dengan memeriksa ZKPs.

- *The server homomorphically* mengkombinasikan *ballot* dan menerbitkan hasil perhitungan yang telah dienkrip dan siapapun dapat mengecek bahwa perhitungan dilakukan dengan benar

ISBN: 978-602-60581-0-2

- Server menyerahkan penghitungan terenkripsi untuk masing-masing *trustee*, dan memperoleh bagian dari kunci dekripsi ciphertext tertentu, bersama dengan bukti bahwa *shared key* terbentuk dengan baik.

- Server mendekrip hasil perhitungan dan menerbitkan hasil. Siapapun dapat mengecek proses dekripsi ini.

Teori Equational. Menggunakan sebuah tandatangan dimana penc (*X*pk*; X*rand*; X*text) menyatakn enkripsi dengan kunci *X*pk dan random Xrand dari plaintext Xtext dan Xciph * Yciph menyatakan kombinasi homomorphic dari cipheretxt Xciph dan Yciph. Menggunakan teori equational dengan +,*,o adalah komutative dan asosiative dan termasuk pada persamaan :

$$\mathsf{dec}(x_{\mathsf{sk}}, \mathsf{penc}(\mathsf{pk}(x_{\mathsf{sk}}), x_{\mathsf{rand}}, x_{\mathsf{text}})) = x_{\mathsf{text}}$$

$$\mathsf{dec}(\mathsf{decKey}(x_{\mathsf{sk}}, ciph), ciph) = x_{\mathsf{plain}} \quad \text{where } ciph = \mathsf{penc}(\mathsf{pk}(x_{\mathsf{sk}}), x_{\mathsf{rand}}, x_{\mathsf{plain}})$$

$$\mathsf{penc}(x_{\mathsf{pk}}, y_{\mathsf{rand}}, y_{\mathsf{text}}) * \mathsf{penc}(x_{\mathsf{pk}}, z_{\mathsf{rand}}, z_{\mathsf{text}}) = \mathsf{penc}(x_{\mathsf{pk}}, y_{\mathsf{rand}} \circ z_{\mathsf{rand}}, y_{\mathsf{text}} + z_{\mathsf{text}})$$

$$\mathsf{checkBallotPf}(x_{\mathsf{pk}}, ballot, \mathsf{ballotPf}(x_{\mathsf{pk}}, x_{\mathsf{rand}}, s, ballot)) = \mathsf{true} \quad \text{where } ballot = \mathsf{penc}(x_{\mathsf{pk}}, x_{\mathsf{rand}}, s)$$

$$\mathsf{checkDecKeyPf}(\mathsf{pk}(x_{\mathsf{sk}}), ciph, dk, \mathsf{decKeyPf}(x_{\mathsf{sk}}, ciph, dk)) = \mathsf{true} \quad \text{where } ciph = \mathsf{penc}(\mathsf{pk}(x_{\mathsf{sk}}), x_{\mathsf{rand}}, x_{\mathsf{plain}}) \text{and } dk = \mathsf{decKey}(x_{\mathsf{sk}}, ciph)$$

Spesifikasi proses pemilihan (Vhelios, Ahelios) didefinisikan [4]:

$$\begin{aligned}
V_{\mathsf{helios}} &\triangleq d(x_{\mathsf{pid}}).\ \overline{d}\langle v\rangle.\ d(x_{\mathsf{ballot}}).\ d(x_{\mathsf{ballotpf}}).\overline{c}\langle\!\langle w, x_{\mathsf{ballot}}, x_{\mathsf{ballotpf}}\rangle\!\rangle\rangle \\
A_{\mathsf{helios}}[_] &\triangleq \nu sk, d.\ (\overline{c}\langle\mathsf{pk}(sk)\rangle \mid (!\nu pid.\ \overline{d}\langle pid\rangle) \mid (!B) \mid T \mid _) \\
B &\triangleq \nu m.\ d(x_{\mathsf{vote}}).\overline{d}\langle\mathsf{penc}(\mathsf{pk}(sk), m, x_{\mathsf{vote}})\rangle. \\
&\quad\ \overline{d}\langle\mathsf{ballotPf}(\mathsf{pk}(sk), m, x_{\mathsf{vote}}, \mathsf{penc}(\mathsf{pk}(sk), m, x_{\mathsf{vote}}))\rangle \\
T &\triangleq c(x_{\mathsf{tally}}).\ \overline{c}\langle\!\langle\mathsf{decKey}(sk, x_{\mathsf{tally}}), \mathsf{decKeyPf}(sk, x_{\mathsf{tally}}, \mathsf{decKey}(sk, x_{\mathsf{tally}}))\rangle\!\rangle
\end{aligned}$$

Individual dan universal verifiability , tes Φ^{IV} dan Φ^{UV} mengarahkan kepada tujuan verifikasi. Dengan demikian, n € N dapat didefinisikan sebagai [4]

$$\begin{aligned}
\Phi^{IV} &\mathrel{\widehat{=}} y =_E \langle\!\langle r_{pid}, r_{ballot}, r_{ballotpf}\rangle\!\rangle \\
\Phi^{UV} &\mathrel{\widehat{=}} z_{\mathsf{tally}} =_E \pi_2(y_1) * \cdots * \pi_2(y_n) \\
&\quad \wedge \textstyle\bigwedge_{i=1}^{n}(\mathsf{checkBallotPf}(x_{\mathsf{pk}}, \pi_2(y_i), \pi_3(y_i)) =_E \mathsf{true}) \\
&\quad \wedge \mathsf{checkDecKeyPf}(x_{\mathsf{pk}}, z_{\mathsf{tally}}, z_{\mathsf{decKey}}, z_{\mathsf{decKeyPf}}) =_E \mathsf{true} \\
&\quad \wedge v_1 + \cdots + v_n =_E \mathsf{dec}(z_{\mathsf{decKey}}, z_{\mathsf{tally}})
\end{aligned}$$

4. Kesimpulan

Jadi dapat disimpulkan bahwa, JCJ/Civitas maupun Helios telah menerapkan metode *individual verifiability, universal verifiability dan eligibility verifiability* dengan protokol dan algoritma masing-masing. Pada dasarnya JCJ/Civitas maupun Helios secara umum mengacu pada sistem yang mengandalkan *universal verifiability* untuk mencapai end-to-end pada *individual verifiability*

ISBN: 978-602-60581-0-2

Daftar Pustaka

[1] Calandrino, J.A., Feldman, A.J., Alex Halderman, J., Wagner, D., Yu, H., Zeller, W.P.: Source code review of the Diebold voting system. In: Report commissioned as part of the California Secretary of State's Top-To-Bottom Review of California Voting Systems. 2007

[2] Ardhana, M.I.G. Peningkatan Anonimitas Dan Verifiabilitas Sistem Pemungutan Suara Melalui Kriptografi Visual, Dissertation Program Doctoral Programs, School of Electrical Engineering and Informatics, Bandung Institute of Technology. 2014

[3] Langer L., Jonker H., Pieters W. Anonymity and Verifiability in Voting: Understanding (Un)Linkability, 12th International Conference, ICICS 2010, Volume 6476 of the series Lecture Notes In Computer Science pp 296-310, Springer

[4] Kremer, S., Ryan, M., Smyth, B. Election Verifiability in Electronic Voting Protocols. In: Gritzalis, D., Preneel, B., Theoharidou, M. (eds.) ESORICS 2010. LNCS, vol. 6345, pp. 389– 404. Springer, Heidelberg

[5] Chaum, D.: Secret-ballot receipts: True voter-verifiable elections. IEEE Security & Privacy 2(1). 2004.

[6] Benaloh, J.: Simple verifiable elections. In: Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, p. 5. USENIX Association, Berkeley

[7] Jakobsson, M., Juels, A., Rivest, R.L.: Making mix nets robust for electronic voting by randomized partial checking. In: Boneh, D. (ed.) USENIX Security Symposium. 2002. pp. 339– 353. USENIX

[8] Kremer, S., Ryan, M., Smyth, B.: Election Verifiability in Electronic Voting Protocols. In: Gritzalis, D., Preneel, B., Theoharidou, M. (eds.) ESORICS 2010. LNCS, vol. 6345, pp. 389– 404. Springer, Heidelberg

[9] Chaum, D., Ryan, P.Y.A., Schneider, S.: A Practical Voter-Verifiable Election Scheme. In: De Capitani di Vimercati, S., Syverson, P.F., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 118–139. Springer, Heidelberg

[10] Adida, B.: Helios: Web-based open-audit voting. In: van Oorschot, P.C. (ed.) USENIX Security Symposium. 2008. pp. 335–348. USENIX Association

[11] Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Atluri, V., De Capitani di Vimercati, S., Dingledine, R. (eds.) WPES. 2005. pp. 61–70.

[12] Bursuc S., Grewal G.S., Ryan M.D., Trivitas: Voters Directly Verifying Votes,Third International Conference, VoteID 2011, Volume 7187 of the series Lecture Notes in Computer Science pp 190-207, Springer

[13] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing University President Using Open-Audit Voting: Analysis of Real-World Use of Helios. In EVT/WOTE'09: Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. USENIX Association, 2009

ISBN: 978-602-60581-0-2

[14] Smyth, Ben; Frink, Steven; Clarkson, Michael R. Election Verifiability: Cryptographic Definitions and an Analysis of Helios and JCJ. Computing and Information Science Technical Reports. Cornell University. 201

[15] David Bernhard, Oliver Pereira, and Bodgan Warinschi. How not to prove yourself: pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In ASIACRYPT'12: *18Th international conference on the theory and Application of Cryptology and Information Security*. 2012 volume 7658 of LNCS, pages 626-643. Springer.

[16] David Bernhard, Veronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. A comprehensive analysis of game-based ballot privacy definitions. Cryptology ePrint Archive, 2015. Report 2015/255 (version 20150319:100626)

ISBN: 978-602-60581-0-2